基于半脆弱水印的图博档视频资源内容认证策略研究*

朱　光[1,2]　丰米宁[1]
[1](南京信息工程大学经济管理学院　南京 210044)
[2](南京大学信息管理学院　南京 210093)

摘要:【目的】设计大数据环境下安全性和实时性更好的半脆弱水印算法，保护图博档视频资源的真实性和完整性。【应用背景】保证视频资源对常规视频操作的鲁棒性，满足图博档视频资源内容认证的实时性需求。【方法】运用量化调制的方法嵌入二值水印图像进行版权验证，在视频关键帧中嵌入索引水印检测帧间篡改，对视频帧的最低有效位进行异或运算生成认证水印检测帧内篡改。【结果】水印算法可以对视频资源进行有效的版权验证和内容认证，透明性较好，对于常规视频操作具有较强的鲁棒性，PSNR 保持在 33 以上。篡改定位时间 5s 左右，具有良好的实时性。【结论】本研究有助于图博档视频资源的真实性和完整性保护，促进大数据环境下图博档信息资源共享和服务融合。

关键词: 图博档　视频资源　内容认证　半脆弱水印　实时性
分类号: G250.76

1　引　言

随着大数据时代的到来，图书馆、博物馆、档案馆等信息资源服务机构纷纷将自身馆藏资源数字化，促进图博档资源的共建共享[1]。受益于多媒体技术的发展和高速宽带网络的普及，生动形象的图博档视频资源成为用户浏览和收藏的首选。然而在大数据共享环境下，一些非法团体为达到某种目的，在没有合法权限的情况下，对图博档视频资源进行恶意篡改和伪造，使得视频内容的真实性和完整性受到严重威胁，给资源原创作者和供应商的合法权益造成极大的侵害。人类由于视觉系统的局限性无法对篡改后的视频资源进行有效的内容认证，而基于哈希函数和密码学的内容认证技术安全性较低，也无法确定视频资源遭受篡改的位置[2]。因此，如何对图博档视频资源进行有效认证成为亟需解决的问题。本文将半脆弱水印技术应用于图书馆、博物馆和档案馆数字视频资源的内容认证中，结合图博档视频资源的特征，针对大数据环境的实时性需求，提出一种结合 DCT(Discrete Cosine Transform)量化系数和最低有效位(Least Significant Bit, LSB)扰动的半脆弱水印算法，有效地解决了现有认证技术在鲁棒性和实时性上的不足，为数字视频资源的内容认证提供了新的应对思路。

2　研究现状

数字水印技术是一种新兴的信息安全技术，通过频域变换将标识信息(即数字水印)嵌入至数字资源中[3]。目前数字水印技术在图博档等机构的研究主要集中在版权保护领域[4-8]，该类水印称为鲁棒水印。在图博档视频资源的内容认证过程中，根据认证目的不同，可以分为“完全级认证”和“内容级认证”两类。“完全级认

通讯作者: 朱光，ORCID: 0000-0003-4749-8603，E-mail: guangguang4992@sina.com。

*本文系国家社会科学基金重大项目“图书、博物、档案数字化服务融合研究”(项目编号: 10&ZD134)、国家自然科学基金项目“信息生命周期视角下的大数据隐私风险评估和溯源问责机制研究”(项目编号: 71503133)和国家社会科学基金项目“数字档案安全及长期保存策略研究”(项目编号: 13CTQ050)的研究成果之一。

证”要求对视频的任何数据部分均不允许更改，检测系统对视频资源的任何轻微改动都做出拒绝判断；而“内容级认证”则强调保护视频所传递的信息，而不是具体表现形式。因此，对于任何保持资源内容的操作，检测系统都认为是可接受的更改，而不会做出拒绝判断[9]。图博档视频资源认证属于“内容级认证”，在网络传播和共享过程中会经历格式转换、有损压缩等操作，要求水印在对这些操作保持一定鲁棒性的前提下，可以较敏感地检测到恶意篡改和内容的替换。这类水印比完全脆弱性水印鲁棒性稍强，称为半脆弱水印[10]。

已有学者对半脆弱水印技术展开了相关研究：Qi 等[11]提出一种图像内容认证策略，通过修改奇异值量化系数的编码实现半脆弱水印信息的嵌入；Ono 等[12]提出一种针对二维条码的半脆弱水印认证算法，将水印标识嵌入至条码图像的中高频小波系数中，检测系数改动以实现条码内容认证；Shi 等[13]提出一种基于运动目标的水印视频内容认证方案，将视频帧的索引号作为可逆水印用于检测时域篡改，再将视频帧的内容轮廓信息和运动目标细节作为另一个水印标识嵌入到视频帧中，用于篡改的检测及篡改内容的定位；Masoumi 等[14]利用 CDMA 技术把水印嵌入到视频运动场景的小波中频系数中，水印信息的更改可以检测恶意的内容篡改；Horng 等[15]对数字视频的时域特性进行分析，将视频在 H.264/AVC 压缩编码过程中的帧内或帧间的预测模式作为特征序列，并将该特征序列作为认证水印嵌入至视频的压缩码流；赵春晖等[16]提出一种基于分块压缩感知的半脆弱零水印算法，将图像划分为若干子块，根据压缩感知理论对各个图像块进行观测，并将观测的特征值作为半脆弱零水印信息保存。

综上，现有的半脆弱水印认证策略研究主要集中在数字图像领域，大多数的视频半脆弱水印算法复杂度较高，难以满足大数据环境下视频内容认证的实时性要求，不利于在图书馆、博物馆和档案馆等机构进行推广和应用。同时，现有算法并没有考虑到图博档视频资源分辨率低、格式固定、数据量小的特点，应用领域并不具有针对性。因此，本文在相关研究的基础上，从算法有效性和实时性的角度出发，提出一种基于 DCT 量化系数和最低有效位扰动的半脆弱视频水印算法，采用量化调制的方法嵌入二值水印标识以确定版权归属，在视频关键帧(I 帧)中嵌入能够检测帧间篡改的索引水印，对视频帧的最低有效位进行异或运算生成检测帧内篡改的认证水印，从而对图博档视频资源的真实性和完整性进行认证。

3 算法设计

图博档视频资源遭受的恶意篡改主要包括空间域篡改和时间域篡改。前者是指对视频帧图像内容的恶意篡改和攻击，时间域篡改指视频帧删除、帧重组以及帧替换等时间轴上的恶意攻击[17]。因此，本文需嵌入三类水印，第一类二值水印图像用来明确版权归属，第二类索引水印用于帧间篡改定位，第三类认证水印用于帧内篡改定位。算法流程如图 1 所示。

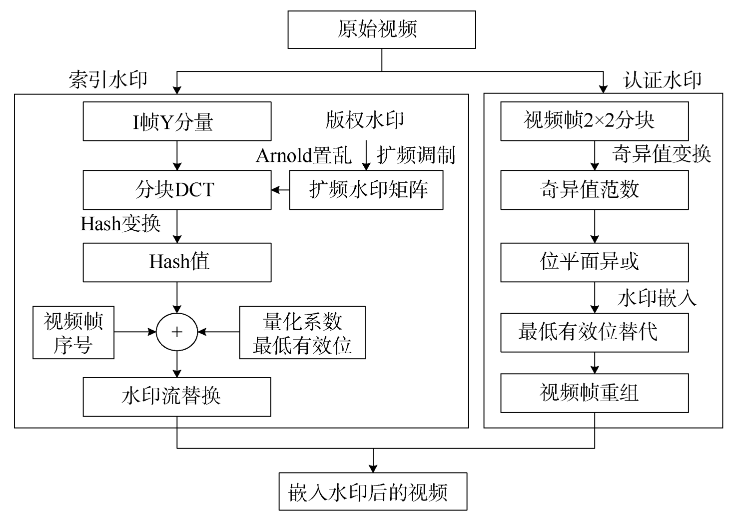


图 1 算法流程图

3.1 水印嵌入

首先嵌入二值水印图像对图博档视频资源进行版权认证，以及嵌入索引水印对图博档视频资源的帧间篡改进行认证和定位，索引水印信息通过DCT系数的Hash 值和视频帧序号来判断是否存在时间域上的攻击和篡改，具体步骤如下：

(1) 获取原始视频关键帧的亮度分量，并对其进行8×8分块的DCT变换，获取相应的DCT系数；

(2) 对二值水印图像进行Arnold置乱(密钥为 K_1)以保证水印信息的安全性，并将置乱后的图像映射为二值水印序列，利用扩频系数将一维水印序列映射为扩频水印矩阵，再对其进行8×8分块的DCT变换；

(3) 利用量化调制的方法嵌入水印信息[18]，并计算嵌入水印后视频帧DCT系数的Hash值，当视频内容遭受恶意篡改和攻击时，DCT 系数会发生变化，从而引起Hash值的改变；

(4) 利用密钥 K_2 从8×8分块中选取一个量化系数，并提取这一系数的最小有效位，将最低有效位、Hash 值和视频帧序号进行组合，用此组合位流替换分块量化系数的最低有效位，完成索引水印信息的嵌入。

嵌入认证水印用于视频资源的帧内篡改定位，具体过程如下。

(1) 选取原始视频帧图像，对其进行2×2分块，定义为 $\mathbf{B}_q=\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix}$，$x_i$ 为像素值。对各子图像块像素值的最低有效位(LSB)置零，得到 $\mathbf{B}'_q=\begin{bmatrix} x'_1 & x'_2 \\ x'_3 & x'_4 \end{bmatrix}$。

(2) 根据奇异值扰动定理，对图像块奇异值范数进行异或运算产生水印信息[19]。首先计算图像块的奇异值范数并取整，如公式(1)所示。其中，f为向下取整函数。

$$N_m = f\left(\sqrt{\sum_{i=1}^{2}\sigma_i^2}\right) \qquad (1)$$

(3) 对 N_m 的 8 个位平面进行异或运算产生水印信息，水印信息与每个分块像素紧密联系，有利于增强水印信息对恶意篡改的敏感性，规则如公式(2)所示。其中 b_i 是 N_m 的第 i 比特位，w_f 是产生的水印信息，w_{f_i} 是水印的第 i 比特像素值。

$$\begin{aligned} & w_{f_1}=b_1\oplus b_2\oplus b_3 \\ & w_{f_2}=b_2\oplus b_3\oplus b_4 \\ & w_{f_3}=b_4\oplus b_5\oplus b_6, w_f=\begin{bmatrix} w_{f_1} & w_{f_2} \\ w_{f_3} & w_{f_4} \end{bmatrix} \\ & w_{f_4}=b_6\oplus b_7\oplus b_8 \end{aligned} \qquad (2)$$

(4) 将水印信息嵌入至对应子图像块像素的最低有效位上，并对各子图像块进行重组得到嵌入水印信息后的视频帧图像。

3.2 水印提取和认证

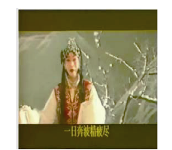
(1) 提取嵌入水印信息的视频关键帧的亮度分量，并对其进行8×8分块的DCT变换；

(2) 根据密钥 K_2 计算 8×8 分块中的 DCT 量化系数，提取对应系数的最低有效位流，包括DCT系数的Hash 值、帧序号和原DCT量化系数的最低有效位。对量化系数进行DCT逆变换，并利用密钥 K_1 对水印序列进行 Arnold 逆置乱，得到提取的二值水印图像，用于版权认证。与此同时，若提取的 Hash 值和原始 Hash 值相等，证明视频资源没有遭到恶意篡改；若两个Hash值不相等，则根据提取的帧序号判断每两个关键帧之间是否存在帧删除、帧添加、帧替换等操作。

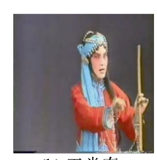
提取用于视频帧内篡改定位的认证水印信息，首先对嵌入水印的视频帧图像进行2×2分块，获取子图像块中各像素值的最低有效位数值，定义为 $\boldsymbol{l}=\begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix}$。与嵌入步骤相同，对子图像块进行奇异值变换、范数取整、像素值异或等操作提取出认证水印 w_f。将 w_f 与 $\boldsymbol{l}$ 进行对比，若完全一致，则视频帧图像没有被篡改；若有数值不一致，则代表视频帧图像遭受篡改，并标记篡改的位置。

4 实验结果及分析

以Matlab 2010为仿真实验平台，对多组视频资源进行水印算法的有效性验证。选取具有代表性的南京图书馆视频资源库中的京剧视频“桃花酒店”、“玉堂春”、“华山情仇”、“侯门之女”，南京博物院视频展示中的“云锦馆”、“珍宝馆”、“漆器馆”，以及南通博物苑馆藏展览中的“四足熏炉”、“观音坐像”、“白砂茶壶”共 10 组视频为测试视频，视频格式为 WMV，视频帧截图如图 2 所示。



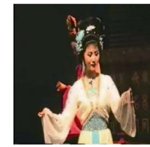
(a) 桃花酒店



(b) 玉堂春



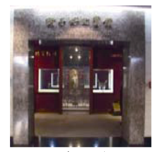
(c) 华山情仇



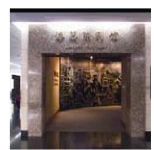
(d) 侯门之女



(e) 云锦馆



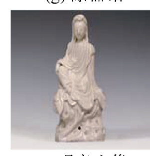
(f) 珍宝馆



(g) 漆器馆



(h) 四足熏炉



(i) 观音坐像



(j) 白砂茶壶

图 2　测试视频

4.1　安全性分析

水印算法安全性的高低取决于密钥，而不依赖于算法。本文运用密钥 K_1 进行 Arnold 置乱，在不知晓 K_1 的情况下，无法获取正确的水印图像。利用密钥 K_2 选择量化系数，恶意攻击者在不知晓 K_2 的情况下无法进行水印攻击。因此本文设计的半脆弱水印算法的安全性完全依赖于密钥 K_1 和 K_2，算法流程可以全部公开。

4.2　可行性分析

半脆弱水印认证算法的可行性分析包括虚警概率分析和漏警概率分析[20]。虚警概率是指待检测视频没有发生篡改，检测结果却显示有篡改发生。由本文算法可知，当待检测视频帧图像的任一子图像块的最低有效位没有发生变化时，提取出的水印和原始水印信息相同。因此，算法的虚警概率 $P_{FA}=0$。

漏警概率是指待检测视频资源发生篡改，但检测结果却没有显示。对于提取的水印信息 $\mathbf{w}_{f'}=\begin{bmatrix} w_{f_1'} & w_{f_2'} \\ w_{f_3'} & w_{f_4'} \end{bmatrix}$ 和提取的 LSB 位 $\boldsymbol{l}=\begin{bmatrix} l_1 & l_2 \\ l_3 & l_4 \end{bmatrix}$ 来说，$P(w_{f_i}=0)=P(w_{f_i}=1)=1/2$ 和 $P(l_i=0)=P(l_i=1)=1/2$。要判定视频没有遭到篡改，要求 $w_{f_i}=l_i\ (i=1,2,3,4)$ 成立。因此，一个被篡改的 2×2 视频帧图像被检测没有遭受篡改的概率为 2^{-4}。若一幅待检测帧图像有 m 个 2×2 子图像块，则漏警概率 $P_M=2^{-4m}$。恶意篡改的图像块太少无法达到其目的，当 m 足够大时，算法的漏警概率足够小，可以忽略。

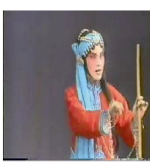
4.3　透明性分析

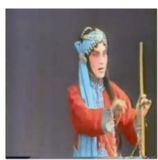
为进一步验证本文水印方案在图博档视频资源内容认证中的有效性，需要对算法的透明性、鲁棒性、篡改定位效果和实时性进行对比分析。透明性是指图博档视频资源在嵌入水印信息的前后，其视觉质量不能有显著下降。透明性的客观评价指标采用峰值信噪比(Peak Signal-to-Noise Ratio, PSNR)，其值越高，透明性越好。若 I(i, j) 表示某一原始视频帧，I′(i, j) 表示嵌入水印后的视频帧，则 PSNR 的计算公式为[21]:

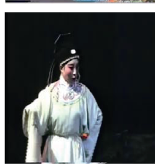
$$PSNR=10lg\frac{MN\max[(I(i,j))^2]}{\sum_{i=1}^{M}\sum_{j=1}^{N}[I(i,j)-I'(i,j)]^2} \tag{3}$$



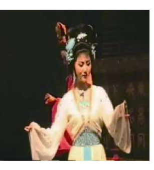


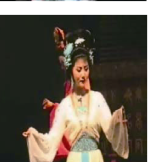


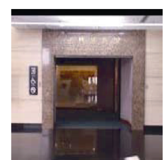


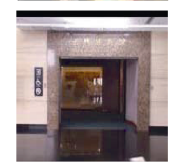












(a) 原始视频　　(b) 嵌入水印后的视频

图 3　透明性分析

图 3 显示了嵌入水印前后视频第 7 帧显示的图像，可以看出水印嵌入前后视频质量没有受到显著影响，人眼视觉系统无法感知水印信息的存在。

表 1 给出 10 组测试视频的 PSNR 值，本文水印算法与文献[11-12]水印算法的透明性对比结果如图 4 所示，可以看出本文算法的透明性更好。

表 1　测试视频的 PSNR 值

测试视频	PSNR
a	33.86
b	34.01
c	33.97
d	34.12
e	33.26
f	33.54
g	34.23
h	33.49
i	33.71
j	34.28

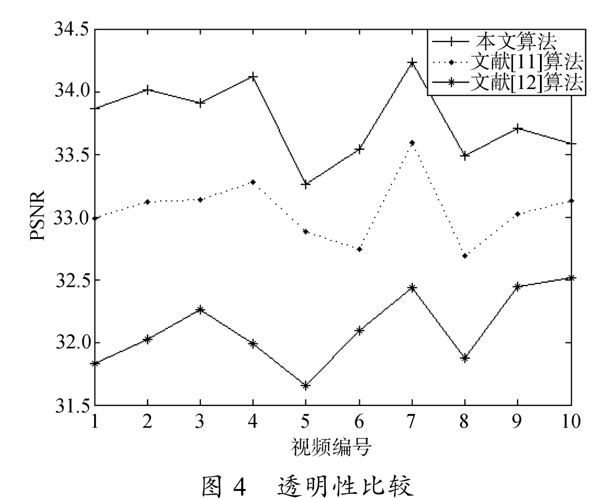


图 4　透明性比较

4.4　鲁棒性分析

本文设计的半脆弱视频水印认证算法属于“内容级认证”，因此需要对网络传播和共享过程中的添加噪声、MPEG 压缩、滤波处理等操作保持一定的鲁棒性。鲁棒性是指经过常规视频操作后，嵌入水印的图博档视频资源仍能提取出清晰的水印标识，以验证版权归属[22]。鲁棒性的评价指标为相关系数(Normalized Correlation，NC)，是指原始水印图像与提取水印图像的相似度。定义 W(i, j) 为原始水印图像，W′(i, j) 表示提取出的水印图像，则 NC 的计算公式为:

$$NC=\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}W(i,j)W'(i,j)}{\sum_{i=1}^{M}\sum_{j=1}^{N}[W(i,j)]^2} \tag{4}$$

选取常见的 10 种视频操作来验证本文算法的鲁棒性，攻击类型如表 2 所示，10 组测试视频受到不同攻击后的相关系数如表 3 所示。以测试视频“桃花酒店”为例，遭受视频攻击后，仍可以提取较清晰的水印图像，如图 5 所示，实验结果表明，本文设计的视频水印算法对 MPEG 压缩、滤波、噪声攻击等常见的视频操作具有较强的鲁棒性。

表 2　操作类型

编号	攻击	编号	攻击
1	MPEG 压缩(QF=90%)	6	添加高斯噪声(σ=0.04)
2	MPEG 压缩(QF=75%)	7	添加高斯噪声(σ=0.06)
3	MPEG 压缩(QF=50%)	8	添加高斯噪声(σ=0.08)
4	MPEG 压缩(QF=30%)	9	3×3 高斯滤波
5	添加高斯噪声(σ =0.02)	10	3×3 中值滤波

表 3　视频操作后水印图像的相关系数

	操作编号									
视频	1	2	3	4	5	6	7	8	9	10
a	0.993	0.982	0.933	0.896	0.877	0.841	0.826	0.803	0.955	0.941
b	0.996	0.969	0.921	0.889	0.863	0.833	0.808	0.805	0.943	0.935
c	0.989	0.972	0.934	0.891	0.872	0.829	0.819	0.794	0.951	0.924
d	0.992	0.968	0.929	0.886	0.851	0.831	0.828	0.809	0.949	0.939
e	0.988	0.987	0.933	0.899	0.879	0.828	0.817	0.805	0.940	0.942
f	0.994	0.959	0.919	0.885	0.882	0.838	0.821	0.812	0.955	0.940
g	0.993	0.964	0.932	0.893	0.880	0.842	0.812	0.812	0.939	0.931
h	0.991	0.971	0.927	0.884	0.883	0.841	0.827	0.801	0.948	0.926
i	0.985	0.983	0.929	0.895	0.872	0.832	0.810	0.811	0.951	0.947
i	0.987	0.985	0.918	0.881	0.880	0.826	0.808	0.797	0.936	0.929

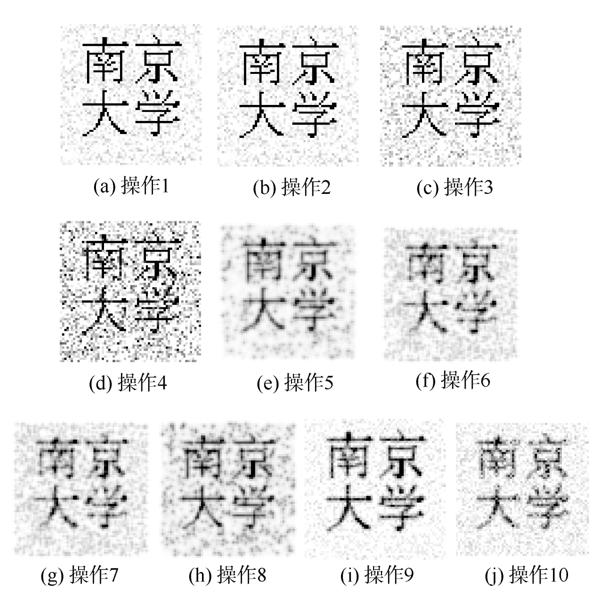


图 5　视频操作后提取的水印图像

以测试视频“桃花酒店”为例，比较本文方法与文献[11-12]水印算法的鲁棒性，如图 6 所示。实验结果表明，本文算法具有较高的鲁棒性。

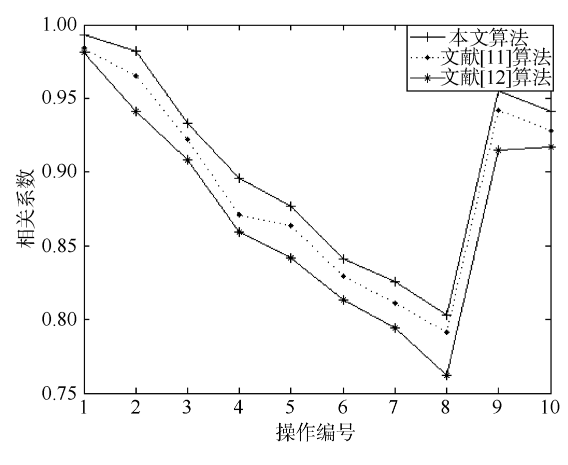


图 6　鲁棒性比较

4.5　篡改定位分析

恶意篡改一般是指对原始视频的帧删除、帧替换及视频帧内容的修改等攻击。视频帧删除和视频帧替换等时间域上的攻击可以通过视频帧序号来进行判断和定位，定位结果如图 7 所示。

以测试视频“侯门之女”为例，针对图博档视频资源的空间域篡改(帧内容篡改)定位进行分析，恶意篡改后的视频帧和原始视频帧在视觉效果上没有差别，篡改定位结果如图 8 所示。



图 7　时间域恶意篡改的定位结果

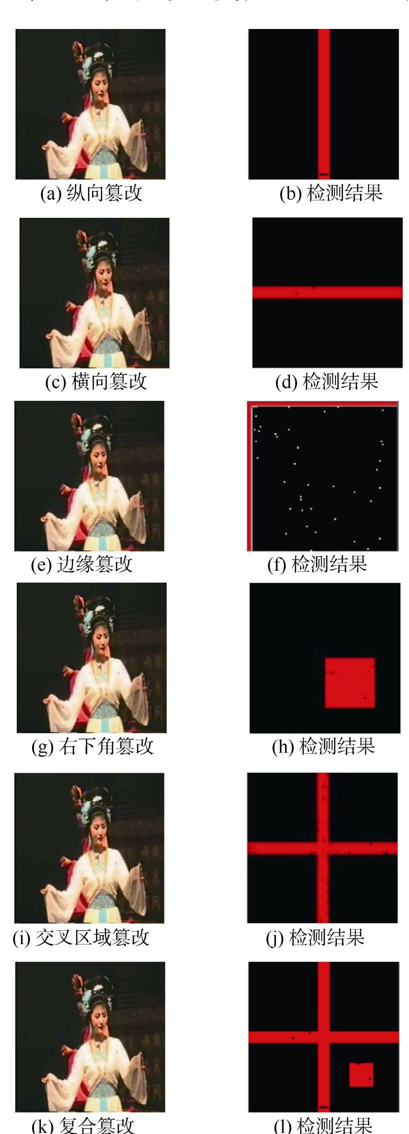


图 8　空间域恶意篡改的定位结果

4.6　实时性分析

计算 10 组测试视频篡改定位的平均时间，与文献[11-12]进行比较，实验结果如表 4 所示，结果表明本

文算法具有更好的实时性，更适合在大数据环境下应用实现。

表 4　视频篡改定位的实时性分析

篡改类型	定位时间/s		
	本文算法	文献[11]算法	文献[12]算法
纵向篡改	4.324	5.146	4.833
横向篡改	4.621	5.326	5.502
边缘篡改	5.134	5.856	5.483
右下角篡改	4.232	4.753	4.494
交叉区域篡改	5.543	6.097	5.886
复合篡改	5.837	6.301	6.021

5　结　语

针对大数据共享环境下图博档视频资源真实性和完整性的内容认证需求，本文设计了一种半脆弱水印算法，通过嵌入版权水印、索引水印和认证水印对数字视频进行版权验证和篡改定位。理论分析和仿真实验结果表明，本文提出的视频水印算法具有较高的安全性和可行性，对常见的视频操作具有较强的鲁棒性，在不降低视频视觉效果的前提下，可以对其进行有效的内容认证。与此同时，较低的复杂度可以支持算法在大数据环境下实时应用。基于此，本文提出的内容认证策略有助于图博档视频资源的真实性和完整性保护，促进大数据环境下图博档信息资源共享和服务融合。

尝试设计可以应用于多种视频格式的通用视频水印算法，引入 Web Service 体系和智能代理(Agent)技术避免重复开发是今后进一步研究的内容。

参考文献：

[1] 朱学芳. 图博档信息资源数字化建设及服务融合探讨[J]. 情报资料工作, 2011(5): 57-60. (Zhu Xuefang. On the Digitalized Construction and Service Integration of the Information Resources of Libraries, Museums and Archives [J]. Information and Documentation Services, 2011(5): 57-60.)

[2] Yu Y H, Zhang L. Research on a Provable Security RFID Authentication Protocol Based on Hash Function [J]. Journal of China Universities of Posts and Telecommunications, 2016, 23(2): 31-37.

[3] Liu H, Xiao D, Zhang R, et al. Robust and Hierarchical Watermarking of Encrypted Images Based on Compressive Sensing[J]. Signal Processing: Image Communication, 2016, 45: 41-51.

[4] 郝世博, 朱学芳. 面向图博档的分块压缩感知图像零水印算法[J]. 现代图书情报技术, 2014(6): 87-93. (Hao Shibo, Zhu Xuefang. An Image Zero-Watermarking Algorithm Using Block Compressive Sensing for Libraries, Museums and Archives [J]. New Technology of Library and Information Service, 2014(6): 87-93.)

[5] 朱光. 基于零水印的图博档彩色图像资源版权保护策略研究[J]. 现代图书情报技术, 2015(12): 89-94. (Zhu Guang. Copyright Protection Scheme of Color Images for Libraries, Museums and Archives Based on Zero-Watermarking [J]. New Technology of Library and Information Service, 2015(12): 89-94.)

[6] 张军亮, 朱学芳. 基于二值图像水印的古籍数字化图像版权保护及其实现[J]. 现代图书情报技术, 2010(9): 79-83. (Zhang Junliang, Zhu Xuefang. The Implementation of Copyright Protection for Digitalizing Ancient Books Image Based on Binary Image Watermarking[J]. New Technology of Library and Information Service, 2010(9): 79-83.)

[7] 朱学芳. 数字档案信息开发及应用管理中的图像水印保护技术[J]. 档案学通讯, 2010(5): 72-75. (Zhu Xuefang. Application of Image Watering in Digital Archives Development[J]. Archives Science Bulletin, 2010(5): 72-75.)

[8] Loukhaoukha K, Refaey A, Zebbiche K. Comments on "Homomorphic Image Watermarking with a Singular Value Decomposition Algorithm"[J]. Information Processing & Management, 2016, 52(4): 644-645.

[9] 陈明奇, 钮心忻, 杨义先. 数字水印的研究进展和应用[J]. 通信学报, 2001, 22(5): 71-79. (Chen Mingqi, Niu Xinxin, Yang Yixian. The Research Developments and Applications of Digital Watermarking [J]. Journal of China Institute of Communications, 2001, 22(5): 71-79.)

[10] Xu D W, Wang R D, Shi Y Q. An Improved Reversible Data Hiding-Based Approach for Intra-frame Error Concealment in H.264/AVC[J]. Journal of Visual Communication and Image Representation, 2014, 25 (2): 410-422.

[11] Qi X J, Xin X. A Singular-value-based Semi-fragile Watermarking Scheme for Image Content Authentication with Tamper Localization[J]. Journal of Visual Communication and Image Representation, 2015, 30:312-327.

[12] Ono S, Maehara T, Minami K. Coevolutionary Design of a Watermark Embedding Scheme and an Extraction Algorithm for Detecting Replicated Two-dimensional Barcodes [J]. Applied Soft Computing, 2016, 46: 991-1007.

[13] Shi Y J, Qi M, Yi Y G, et al. Object Based Dual Watermarking for Video Authentication [J]. Optik, 2013, 124(19): 3827-3834.
[14] Masoumi M, Amisi S. Content Protection in Video Data Based on Robust Digital Watermarking Resistant to Intentional and Unintentional Attacks [J]. International Arab Journal of Information Technology, 2012, 11(2): 204-212.
[15] Horng S J, Farfoura M E, Fan P Z, et al. A Low Cost Fragile Watermarking Scheme in H.264/AVC Compressed Domain [J]. Multimedia Tools and Applications, 2014, 72(3): 2469-2495.
[16] 赵春晖, 刘巍. 基于分块压缩感知的图像半脆弱零水印算法[J]. 自动化学报, 2012, 38(4): 609-617. (Zhao Chunhui, Liu Wei. Block Compressive Sensing Based Image Semi-fragile Zero-watermarking Algorithm [J]. Acta Automatica Sinica, 2012, 38(4): 609-617.)
[17] 李淑芝, 张翔, 邓小鸿, 等. 基于模式特征的 H.264/AVC 可逆视频水印[J]. 中国图象图形学报, 2015, 20(10): 1285-1296. (Li Shuzhi, Zhang Xiang, Deng Xiaohong, et al. Reversible Video Watermarking Algorithm for H.264/AVC Based on Mode Feature [J]. Journal of Image and Graphics, 2015, 20(10): 1285-1296.)
[18] Ghazy R A, Amoon M, Abdallah H A, et al. Block Based Embedding of Encrypted Watermarks Using Singular Value Decomposition [J]. Optik, 2014, 125(20): 6299-6304.
[19] Rastia P, Samieib S, Agoyic M, et al. Robust Non-Blind Color Video Watermarking Using QR Decomposition and Entropy Analysis [J]. Journal of Visual Communication and Image Representation, 2016, 38: 838-847.
[20] Dutta T, Gupta H P. A Robust Watermarking Framework for High Efficiency Video Coding (HEVC) – Encoded Video with Blind Extraction Process [J]. Journal of Visual Communication and Image Representation, 2016, 38: 29-44.
[21] Lu Z M, Zheng W M, Pan J S, et al. Multi-Purpose Image Watermarking Method Based on Mean-Removed Vector Quantization [J]. Journal of Information Assurance and Security, 2006, 1(1): 33-42.
[22] 蒋刚毅, 李文锋, 郁梅, 等. H.264/AVC 压缩域鲁棒视频水印[J]. 光学精密工程, 2015, 23(1): 260-270. (Jiang Gangyi, Li Wenfeng, Yu Mei, et al. Robust Video Watermarking in H.264/AVC Compressed Domain [J]. Optics and Precision Engineering, 2015, 23(1): 260-270.)

作者贡献声明:

朱光: 算法设计, 论文撰写;
丰米宁: 论文修改, 数据整理。

利益冲突声明:

所有作者声明不存在利益冲突关系。

支撑数据:

支撑数据见期刊网络版 http://www.infotech.ac.cn。
[1] 朱光. 程序代码.txt. 水印算法相关代码.
[2] 朱光, 丰米宁. 透明性比较数据.xls. 透明性实验数据.
[3] 朱光, 丰米宁. 鲁棒性比较数据.xls. 鲁棒性实验数据.
[4] 朱光, 丰米宁. 实时性比较数据.xls. 实时性实验数据.

收稿日期: 2016-10-17
收修改稿日期: 2016-11-02

Content Authentication for Video Resources of Libraries, Museums and Archives with Semi-fragile Watermarking

Zhu Guang[1, 2] Feng Mining[1]
[1] (School of Economics and Management, Nanjing University of Information Science & Technology, Nanjing 210044, China)
[2](School of Information Management, Nanjing University, Nanjing 210093, China)

Abstract: [**Objective**] This study designs a more secure semi-fragile watermarking algorithm for the big data environment, which protects the authenticity and integrity of online video resources of libraries, museums and archives (LAM). [**Context**] The algorithm improves the robustness of video resources in normal operation, and then meets the real-time demand of content authentication. [**Methods**] First, we embedded the binary watermarking image to the videos with the help of quantization modulation to protect their copyright. Second, we inserted the index watermarking into key frames of videos to detect the inter-frame modifications. Finally, we generated the authentication watermarking with XOR operation of least significant bit to detect the intra-frame tampers. [**Results**] The proposed algorithm was robust and transparent in normal operations, and its value of Peak Signal to Noise Ratio was above 33. The time of tamper localization was around 5 seconds. [**Conclusions**] The proposed algorithm protects the authenticity and integrity of LAM videos, and then promotes the information sharing and service integration.

Keywords: LAM Video resources Content authentication Semi-fragile watermarking Timeliness